

ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations. In one embodiment, an apparatus is provided for performing cryptographic operations. The apparatus includes a cryptographic instruction, keygen logic, and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of the one of the cryptographic operations. The keygen logic is operatively coupled to the cryptographic instruction. The keygen logic directs the computing device to expand the provided cryptographic key into the corresponding key schedule. The execution logic is coupled to the keygen logic. The execution logic expands the provided cryptographic key into the corresponding key schedule.